



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/004,126	12/04/2001	Andrew Duke	10001-30614	8033

22930 7590 11/30/2004

HOWREY SIMON ARNOLD & WHITE LLP
ATTEN: MARGARET P. DROSOS, DIRECTOR OF IP ADMIN
2941 FAIRVIEW PARK DR, BOX 7
FALLS CHURCH, VA 22042

EXAMINER

EHICHIOYA, FRED I

ART UNIT

PAPER NUMBER

2162

DATE MAILED: 11/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

TW

Office Action Summary	Application No. 10/004,126	Applicant(s) DUKE ET AL.	
	Examiner Fred I. Ehichioya	Art Unit 2162	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 September 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1 - 15, and 17 - 20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 2-4 is/are allowed.
- 6) ☒ Claim(s) 1, 5 - 15, and 17 - 20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☒ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. Applicants arguments, with respect to claims 1, 5, 6 and 8 – 15 filed September 29, 2004 have been fully considered but they are not persuasive for the following reasons.

Applicants argue: "Wallner fails to disclose associating each non-leaf node with a corresponding set of keys where each key in the corresponding set of keys further corresponds to at least one child node of the non-leaf node as recited by claims 1, 5, 6 and 8 – 15 and a plurality of sets of associated keys where the set of associated keys comprises keys associated with subsets of child nodes of a non-leaf node as recited by claims 17 - 19" (page 9, paragraph 2).

Regarding applicants' argument: Examiner respectfully disagrees with the applicants. Applicant's Admitted Prior Art (hereinafter "APA") discusses these limitations as shown in prior art figs. 1, 2 and also shown on page 2, lines 11 – 15 of the specification "As shown in FIG. 1, this method is based . . . would hold the keys associated with each node on the path from the root to that user".

2. Examiner respectfully disagrees with all of the allegations as argued. Examiner in his previous office action pointed out the exact locations in the cited prior art. In view of the above, the examiner contends that all limitations as recited in the claims have been addressed in this Office Action. For the above reasons, Examiner believed that rejection of the last Office action was proper.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1, 17, 18 and 20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. There is no mention as to “defining at least one non-leaf node positioned between the root node and leaf node, said non-leaf node having a parent node and a child node”, and therefore is not enabling to one of ordinary skill in the art.

Regarding claims 5 - 15, these claims depend from claim 1 and claims 18 and 19 depend from claim 17; therefore inherit their deficiencies respectively.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

5. Claims 1, 5, 6, 8 – 17, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Non-Patent Literature document by D. Wallner et al (hereinafter "Wallner"), Key Management For Multicast: Issues and Architectures", June 1999, The Internet Society, in view of APA.

Regarding claim 1, Wallner teaches a method for storing and updating information in a network having n hierarchical levels, said method comprising the steps of:

defining a root node positioned in a first of said levels, said root node having no parent node and at least one child node (see Fig. 2, where the root node is Key O with no parent node and at least Key M and Key N as child nodes);
defining at least two leaf nodes positioned in an n th of said levels, each of

said leaf nodes having a parent node and no child node (see Fig. 2, where Key M and Key N are leaf node and n level is first level);

defining a corresponding path between each of said at least two leaf nodes and said root node (see Fig.2, where each of said at least two leaf nodes and said root node are Key M – Key O or Key N – Key O); and

providing each leaf node with a related set of keys wherein said related set of keys includes each key associated with each non-leaf node on said corresponding path from said leaf node to said root node (see Fig. 2, section 5.4.1 pages 14 and 15).

Wallner does not explicitly teach defining at least one non-leaf node positioned between the root node and leaf node, said non-leaf node having a parent node and a child node; and

associating each non-leaf node with a corresponding set of keys wherein each key in said corresponding set of keys further corresponds to at least one child node of said non-leaf node.

APA teaches defining at least one non-leaf node positioned between the root node and leaf node, said non-leaf node having a parent node and a child node (see figs. 1 and 2; wherein the non-leaf node is positioned between root node and leaf node. The root node and the leaf node are the parent and child nodes respectively).

associating each non-leaf node with a corresponding set of keys wherein each key in said corresponding set of keys further corresponds to at least one child

node of said non-leaf node (see figs. 1, 2 and also shown on page 2, lines 11 – 15 of the specification “As shown in FIG. 1, this method is based . . . would hold the keys associated with each node on the path from the root to that user”).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine teaching of APA with the teaching of Wallner wherein sending a new key to each authorized user every time the system need to be updated is eliminated. The motivation is that “this system reduces the number of messages that the broadcast needs to send when the system is updated”.

Regarding claim 5, Wallner teaches each non-leaf node is associated with more than two child nodes (see Fig. 2, where Key I is a non-leaf node associated with Key A and Key B).

Regarding claim 6, Wallner teaches each non-leaf node is associated with the same number of child nodes (see Fig. 2, Key I and Key J are non-leaf nodes associated with Key A and Key B and key C and Key D respectively).

Regarding claim 8, Wallner teaches aim 1 further comprising the step of identifying a specific one of said leaf nodes as a compromised leaf node (see page 17, paragraph 1).

Regarding claim 9, Wallner teaches the step of removing at least a portion of said path between said compromised leaf node and said root node (see page 14, paragraph 4).

Regarding claims 10 and 14, Wallner teaches the step of marking a key in said set of keys related to said compromised leaf node as a compromised key (see pages 7 and 8, section 5.1).

Regarding claim 11, Wallner teaches the step of sending a message from said root node to a non-compromised leaf node using a key that has not been marked as a compromised key (see page 15, paragraph 2).

Regarding claim 12, Wallner teaches the step of identifying each of one or more specific leaf nodes as a compromised leaf node (see page 17, paragraph 1).

Regarding claim 13, Wallner teaches the step of removing at least a portion of said path between each of said one or more compromised leaf nodes and said root node (see page 12, section 5.4 and #1).

Regarding claim 15, Wallner teaches the step of sending a message from said root node to a non-compromised leaf node using a key that has not been marked as a compromised key (see page 19, section 5.4.2.4 paragraphs 1 and 2).

Regarding claim 17, Wallner teaches a system for storing and updating information in a network having a plurality of hierarchical levels, comprising:

- a root node associated with a highest of said levels, said root node having at least two child nodes and no parent node (see Fig. 2, where the root node is Key O with no parent node and at least Key M and Key N as child nodes);

- at least two leaf nodes associated with a lowest of said levels, each of said leaf nodes having a parent node and no child node (see Fig.2, Key a and Key B are two leaf nodes associated with a lowest of said levels having parent node Key I but no child node);

- a corresponding path between each of said at least two leaf nodes and said root node (see Fig. 2, corresponding path between each of said at least two leaf nodes and said root node are: Key A – Key I – Key M – Key O or Key B – Key I – Key M – Key O); and

- Wallner does not explicitly teach at least two non-leaf nodes associated with levels between the highest of said levels and the lowest of said levels, each non-leaf node having a parent node and at least two child nodes; and

- a plurality of sets of associated keys, each set of associated keys corresponding to a non-leaf node wherein said set of associated keys comprises keys associated with subsets of child nodes of non-leaf node.

APA teaches at least two non-leaf nodes associated with levels between the highest of said levels and the lowest of said levels, each non-leaf node having a parent node and at least two child nodes (see figs. 1 and 2; wherein the at least two non-leaf

node is between root node (highest levels) and leaf node (lowest levels). The root node and the leaf node are the parent and child nodes respectively); and

a plurality of sets of associated keys, each set of associated keys corresponding to a non-leaf node wherein said set of associated keys comprises keys associated with subsets of child nodes of non-leaf node (see figs. 1, 2 and also shown on page 2, lines 11 – 15 of the specification “As shown in FIG. 1, this method is based . . . would hold the keys associated with each node on the path from the root to that user”).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine teaching of APA with the teaching of Wallner wherein sending a new key to each authorized user every time the system need to be updated is eliminated. The motivation is that “this system reduces the number of messages that the broadcast needs to send when the system is updated”.

Regarding claim 19, Wallner teaches said root node may send a message to at least one leaf node (see page 14, paragraphs 1 and 2).

Regarding claim 20, Wallner teaches a system for storing and updating information in a network having a plurality of hierarchical levels, comprising:

a root node associated with a first of said levels, said root node having no parent node and at least one child node (see Fig. 2, where the root node is Key O with no parent node and at least Key M and Key N as child nodes);

Wallner does not explicitly teach at least one non-leaf nodes associated with a second of said levels, each non-leaf node comprising of a parent node and at least one child node;

at least two leaf nodes associated with a third of said levels, each of said leaf nodes having a parent node and no child node; and

a plurality of set of keys, wherein each set of keys is associated with a non-leaf node and each set of keys further comprises keys associated with subsets of child nodes of the non-leaf node.

APA teaches at least one non-leaf nodes associated with a second of said levels, each non-leaf node comprising of a parent node and at least one child node (see figs. 1 and 2; wherein the non-leaf node is positioned between root node and leaf node. The root node and the leaf node are the parent and child nodes respectively).

at least two leaf nodes associated with a third of said levels, each of said leaf nodes having a parent node and no child node (see fig. 1; wherein 160 – 167 are leaf nodes associated with third level that have parents nodes but no child nodes) and

a plurality of set of keys, wherein each set of keys is associated with a non-leaf node and each set of keys further comprises keys associated with subsets of child nodes of the non-leaf node (see figs. 1, 2 and also shown on page 2, lines 11 – 15 of the specification “As shown in FIG. 1, this method is based . . . would hold the keys associated with each node on the path from the root to that user”).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine teaching of APA with the teaching of Wallner wherein

sending a new key to each authorized user every time the system need to be updated is eliminated. The motivation is that "this system reduces the number of messages that the broadcast needs to send when the system is updated".

6. Claims 7 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wallner in view of APA and further in view of Non-Patent Literature document by David A. McGrew et al (hereinafter "McGrew"), Key Establishment in Large Dynamic Group Using One-Way Function Trees, May 20, 1998, Cryptographic Technologies Group, Glenwood, MD.

Regarding claim 7, Wallner or APA does not explicitly teach internal node McGrew teaches the step of defining an internal node positioned on said corresponding path between said root node and a first of said leaf nodes, said internal node being associated with a hierarchical level between said first level and said nth level (see page 3, section 3.1).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine teaching of McGrew with the teaching of Wallner wherein the each member's knowledge about the current state of the key tree is limited. The motivation is that the invention creates a system where group members communicate with privacy and or authentication.

Regarding claim 18, McGrew teaches at least one internal node on said corresponding path between each of said leaf nodes and said root node, each of said internal nodes having a parent node and at least one child node, each of said internal nodes associated with a further one of said plurality of levels (see pages 3 – 5, sections 3.1, 3.2, 3.3, and 4).

Allowable Subject Matter

7. Claims 2, 3 and 4 are allowable over the prior art of record.

The following is a statement of reasons for the indication of allowable subject matter:

As to claim 2, the prior art of record does not teach or fairly suggest a method for storing and updating information in a network having n hierarchical levels, said method comprising the steps of:

defining a root node positioned in a first of said levels, said root node having no parent node and at least one child;

defining at least two leaf nodes positioned in an n th of said levels, each of said leaf nodes having a parent node and no child node;

defining a corresponding path between each of said at least two leaf nodes and said root node;

associating each non-leaf node with a corresponding set of keys wherein each key in said corresponding set of keys further corresponds to at least one child node of said non-leaf node; and

providing each leaf node with a related set of keys, wherein said corresponding set of keys associated with each non-leaf node includes $2^m - 1$ keys where m is the maximum number of child nodes that may be associated with each non-leaf node.

As to claim 3, the prior art of record does not teach or fairly suggest defining a root node positioned in a first of said levels, said root node having no parent node and at least one child;

defining at least two leaf nodes positioned in an n th of said levels, each of said leaf nodes having a parent node and no child node;

defining a corresponding path between each of said at least two leaf nodes and said root node;

associating each non-leaf node with a corresponding set of keys wherein each key in said corresponding set of keys further corresponds to at least one child node of said non-leaf node; and

providing each leaf node with a related set of keys, wherein said corresponding set of keys associated with each non-leaf node includes $2^m - 2$ keys where m is the maximum number of child nodes that may be associated with each non-leaf node;

As to claim 4, the prior art of record does not teach or fairly suggest defining a root node positioned in a first of said levels, said root node having no parent node and at least one child;

defining at least two leaf nodes positioned in an n th of said levels, each of

said leaf nodes having a parent node and no child node;

defining a corresponding path between each of said at least two leaf nodes and said root node;

associating each non-leaf node with a corresponding set of keys wherein each key in said corresponding set of keys further corresponds to at least one child node of said non-leaf node; and

providing each leaf node with a related set of keys, wherein said related set of keys provided to each leaf node includes $(n-1)*(2^m - 1)$ keys where m is the maximum number of child nodes that may be associated with each non-leaf node.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fred I. Ehichioya whose telephone number is 571-272-4034. The examiner can normally be reached on M - F 8:00 AM to 4:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E. Breene can be reached on 571-272-4107. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Fred I. Ehichioya
Patent Examiner
Art Unit 2162

November 15, 2004



**SHAHID ALAM
PRIMARY EXAMINER**